1. A method for securing data within a wireless database management system, the method comprising the steps of:

Encrypting data transferred within a wireless database management system with a public key method;

Encrypting data transferred within a wireless database management system with a private key method; and

Encrypting data transferred between a wireless base station and a server with a low-layer security protocol.

2. The method of Claim 1 further comprising the step of:

limiting access to a wireless database management system with a firewall between a server and the Internet.

3. The method of Claim 2 further comprising the step of:

limiting access to a wireless database management system with a firewall between a database server and a server.

4. The method of Claim 1 further comprising the step of:

timing out connections between a wireless device and a server.

5. The method of Claim 1 further comprising the step of:

authenticating the identity of a user of a wireless database management system.

6. The method of Claim 1 further comprising the step of:

categorizing users of a wireless database management system into groups that are allowed different levels of access to a database.

7. The method of Claim 1 further comprising the step of:

coding queries made to a database server by a user of a wireless device, and storing those queries and codes in memory.

8. The method of Claim 1 further comprising the step of:

Identifying a session that a user of a wireless device has established with a server with a session identification phrase, and storing the session identification phrase in memory.

9. The method of Claim 4 further comprising the step of:

allowing the timing out of connections between a wireless device and a server to be adjusted.

10. The method of Claim 1 further comprising the step of:

using a controlled wireless proxy server for securing data transferred between a wireless base station and the Internet.

11. The method of Claim 10 further comprising the steps of:

limiting access to a wireless database management system with a firewall between a server and the Internet;

using a controlled server for securing data transferred on the Internet; and
connecting an Intranet to a controlled server on the Internet through the firewall.

12. The method of Claim 11 further comprising the step of:
limiting access to a wireless database management system with a firewall between a database server and a server.

13. The method of Claim 1 further comprising the step of:
compressing and parsing data transferred between a wireless device and a wireless base station.

14. The method of Claim 1 further comprising the step of:
nicknaming the address of a database.

15. The method of Claim 14 further comprising the step of:
storing the nickname and its address in memory.

16. A method for securing data within a wireless database management system, the method comprising the steps of:
authenticating the identity of a user of a wireless database management system;
identifying a session that a user of a wireless device has established with a web server with a session identification phrase, and storing the session identification phrase in memory; and
timing out connections between a wireless device and a server.

17. The method of claim 16 further comprising the step of:
allowing the timing out of connections between a wireless device and a server to be adjusted.

18. The method of claim 16 further comprising the steps of:
encrypting data transferred within a wireless database management system with a public key method;
encrypting data transferred within a wireless database management system with a private key method; and
encrypting data transferred between a wireless base station and a server with a low-layer security protocol.

19. The method of Claim 16 further comprising the step of:
limiting access to a wireless database management system with a firewall between a server and the Internet.

20. The method of Claim 16 further comprising the step of:
limiting access to a wireless database management system with a firewall between a database server and a server.

21. The method of Claim 16 further comprising the step of:
categorizing users of a wireless database management system into groups that are

allowed different levels of access to a database.

22. The method of Claim 16 further comprising the step of:
    coding queries made to a database server by a user of a wireless device, and storing those queries and codes in memory.

23. The method of Claim 16 further comprising the step of:
    using a controlled wireless proxy server for securing data transferred between a wireless base station and the Internet.

24. The method of Claim 23 further comprising the steps of:
    limiting access to a wireless database management system with a firewall between a server and the Internet;
    using a controlled server for securing data transferred on the Internet; and connecting an Intranet to a controlled server on the Internet through the firewall.

25. The method of Claim 24 further comprising the step of:
    limiting access to a wireless database management system with a firewall between a database server and a server.

26. The method of Claim 16 further comprising the step of:
    nicknaming the address of a database.

27. The method of Claim 26 further comprising the step of:
    storing the nickname and its address in memory.

28. The method of Claim 16 further comprising the step of:
    compressing and parsing data transferred between a wireless device and a wireless base station.